**KHLP - Cybersafety For Seniors – Lesson Plan**

Resources: TSS Cybersafety.ppt; Stevie's Scam School\_ Rebate scam.mp4; Outsmart the scammers with The Checkout.mp4

Handouts: Little Black Book; CyberSecurity Readers Digest article.pdf, TSS Handout Cyber Safety.doc

Slide 2, Of Concern

* ACMA: Australian Communications and Media Authority. Link to report is on handout.
* Can’t find any later data but not surprised. Many peoples PC’s that I fix:
  + Out of date or no antivirus (very few with viruses fortunately)
  + Very few had any malware detection, and had a fair bit on the PC
  + Some had the firewall turned off
* **Survey:** Who understand what a firewall does?

Slide 3, We’re in the wrong business

* SCAMwatch – division of ACCC (Australian Competition and Consumer Commission)
* Actual losses would be higher as ACCC is only one of several agencies
* 88% reported no financial loss **(same in 2012)**
* Most common loss in 2010 was $100 to $499 **(same in 2012)**
* Mass marketed advance fee fraud is the highest reported scam > ½ the reports (consist of advance fee/up-front payment, lottery and sweepstakes, unexpected prizes, and dating and romance scams)
* Computer hacking was second (23% of reports) largely due to scam phone calls requesting remote access to ‘fix’ technical problems **(13% in 2012)**
* Reported scams most common in the 25-54 age group (mostly 35-44 in 2012)
* **2012** – 65% increase in online shopping scams ( $4 million)
* **2012** – 56% of all scams via phones, mobile and landlines
* **SURVEY:** How many people subscribe to the SCAMwatch newsletter?

**SHOW VIDEO** Stevies Scam School - Rebates

Slide 4, Allaying Fears

* Phone – would you believe a stranger who said they worked for xxxxx?
* Credit Card – there are card readers out there
* Front door – ‘we’re in the neighbourhood and noticed a couple of cracked tiles…..’.
* Street - ‘We are collecting on behalf of sob, sob sob.
* Relatives – Why wait till she/he has gone. I need it now. Trust me. I’ll look after you.
* Internet is just another communication channel. Not to be feared.

Slide 5, Little Black Book of Scams

Slide 6, Simple Rules

* Common sense, too good to be true; something for nothing.
* My name is Bill Gates. Disprove it please!
* Never tell important passwords to others, including relatives
* When filling in forms only provide the minimum required. Fields usually have an asterisk
* Discuss your proposed deal with others. Shop around
* Sleep on it. Stop and think.
* Get and distribute Scamwatch newsletters; read Black Book and distribute.

Slide 7, Keiths Basic Precautions

* MSE, AVG, Avast, Avira all free and work fine
* **Survey:** Who uses one of the free antivirus programs? Any comments?
* **Survey:** Who can truthfully say their PC is fully patched?
* Link Checker – some antivirus have built in – eg AVG. I use an addin called Web Of Trust (WOT)
* Common sense approach to protection is well explained on the handout.

Slide 8 Password Ideas

* Easily re-creatable rather than commit to memory
* Never a recognisable word
* Mix of characters and case
* **Survey: How many people change their passwords?**
* **QUIZ TIME**
* Jack and Jill went up the hill
* Mary had a little lamb….. Upper case M for Mary, 1 substitutes for l, 5 for S
* John, Mary, tom, catherine and noel live at post code 2756. Note upper case for parents
* Person a’s birthday is 4th December, AND b’s is 13th May

Slide 9, Safe Surfing Tips

* Link Checkers are WOT, AVG
* What’s on the page and where the link ACTUALLY goes are totally different. Sometimes the status bar needs turning on.
* **Question:** Who knows how to kill off a process? (Ctrl+Alt+Esc, Process tab) Or how to shut power off a laptop? (Hold power button in for 7-10 secs)
* **If necessary, Appshare to show.**
* Hoax emails: eg “…It is a virus that opens an Olympic torch that burns the whole hard disc…”. Just highlight a key phrase eg “opens an Olympic torch”. Reliable checks sites are snopes.com, hoax-slayer.com; urbanlegends.about.com; truthorfiction.com; sophos.com
* www.museumofhoaxes.com is worth a browse.
* Gizmos security wizard: <http://www.techsupportalert.com/SecWiz> These are listed on the handout.

Slide 10 Wi-Fi / Cafes

* Always have a password for your home Wi-fi. You can change the default
* Ideally change the Admin password to log onto the router
* Paranoia – consider MAC addressing
* Public access points consider as not secure; possible intercepts
* Avoid financial transactions; banking, buying stuff
* Log out of everything
* Make sure it doesn’t remember passwords. Untick ‘Remember Me’

Slide 11, Sundries

* Do not call register only stops Australian firms. Won’t stop calls from overseas.
* Children are very computer savvy. They will quickly go to sites, download games etc. These can install malware, unwanted search systems and toolbars. At worst are viruses.
* Make sure that your account has a password and that children have their own restricted account
* Handout with some good advice and plenty of links is at www.tinyurl.com/bfsresources

**SHOW VIDEO:** “Outsmart the scammers with ‘The Checkout”